Jamming of NB-IoT Synchronisation Signals

Gabriela Morillo and Utz Roedig

University College Cork, Ireland
{g.morillo,u.roedig}@cs.ucc.ie

Abstract. Narrowband-Internet of Things (NB-IoT) is a relatively novel Low Power Wide Area Network (LPWAN) radio technology used to deploy Internet of Things (IoT) infrastructures at scale. It is important that such deployments are resilient to attacks. In this work we describe how interference on the NB-IoT synchronisation signals - the initial communication steps - can be used to implement an effective Denial of Service (DoS) attack. Interference with the synchronisation prevents communication and may also allow an attacker to force a device to connect with a specific base station.

1 Introduction

Narrowband-Internet of Things (NB-IoT) is a Low Power Wide Area Network (LPWAN) radio technology defined by the 3rd Generation Partnership Project (3GPP) standard, Release-13 [1]. NB-IoT aims to support a large number of low-cost, low energy consumption, and low data rate devices operated in a large enhanced coverage area. NB-IoT is increasingly seen as the preferred future IoT technology as it is deployed as part of the existing Long-Term Evolution (LTE) infrastructure and uses a licensed band that enables reliable and future-proof deployments. NB-IoT provides several security mechanisms based on established mechanisms defined for LTE [2]. However, privacy and security in NB-IoT have yet received little research attention.

In this work we consider an adversary using a jamming device to disrupt NB-IoT communication. We consider an intelligent jammer that targets the initial communication steps of NB-IoT communication to have a maximum impact. Specifically we describe and investigate how a jammer can interfere with the Narrowband Primary Synchronisation Signal (NPSS) and Narrowband Secondary Synchronisation Signal (NSSS) which are used to initiate the NB-IoT contention-based random-access procedure. NPSS and NSSS perform time and frequency synchronisation, cell identity detection and acquisition of frame infrastructure information. NPSS is used to obtain symbol timing and Carrier Frequency Offset (CFO), while NSSS is used to obtain the Narrowband Physical Cell ID (NB-PCID). Interference with NPSS and NSSS can prevent an NB-IoT device to initiate communication with a base station (eNodeB). Furthermore, our experiments indicate that careful design of the interference signal could allow an attacker to force the User Equipment (UE) to recognise a specific NB-PCID.

Existing work has focused on LTE specific attacks. For example, Eygi et al. [3] describe a countermeasure against smart jamming attacks on LTE synchronisation signals. The authors point out the vulnerability of LTE to jamming attacks due to the broadcast nature of the channel. Their work is focused specifically on the LTE downlink synchronisation signals. As countermeasure a jamming detection is proposed based on the Neyman-Pearson theorem. Simulation results show lower jamming success and better cell id detection. Labib et al. [4] describe a mechanism to enhance the immunity of LTE Systems against spoofing. The work analyses spoofing of the LTE synchronisation signal where standard-compliant primary and secondary synchronisation sequences are transmitted by a fake cell. Several mitigation techniques are proposed. The simulation results show that LTE control channel spoofing is an effective DoS attack during the cell selection process.

To the best of our knowledge, there has not yet been an investigation of smart jamming attacks on the synchronisation signals in NB-IoT.

2 The UE and eNodeB Synchronisation Process

The full specification of the NB-IoT protocol was completed in June 2016 and is described in [5]. Here we describe only the synchronisation procedure.

When an NB-IoT device (the UE) becomes active, it synchronises with a base station (eNodeB) to establish a communication link. First, the UE needs to identify a suitable cell to attach to and for this purpose parameters such as symbol, subframe, and frame timing and carrier frequency synchronisation must be obtained.

The NB-IoT random access procedure is illustrated in Figure 1. The process starts with the transmission of the NPSS and NSSS which are used by the UE to perform time and frequency synchronisation, cell identity detection and acquisition frame infrastructure information. The NPSS is used to obtain symbol timing and Carrier Frequency Offset (CFO), while the NSSS is used to obtain the NB-PCID.

After this step, the UE acquires the Master Information Block (MIB) carried by the Narrowband Broadcast Channel (NPBCH) which is transmitted in subframe 0 in every transmitted frame. The MIB provides scheduling information for the uplink and downlink data channels.

Then, the random-access procedure initiates when the UE sends a random access preamble through Narrowband Physical Random Access Channel (NPRACH). Several messages are exchanged between UE and eNodeB through the Narrowband Physical Downlink Shared Channel (NPDSCH) and Narrowband Physical Uplink Shared Channel (NPUSCH) to obtain scheduling information and identity parameters that allow the connection establishment [6].

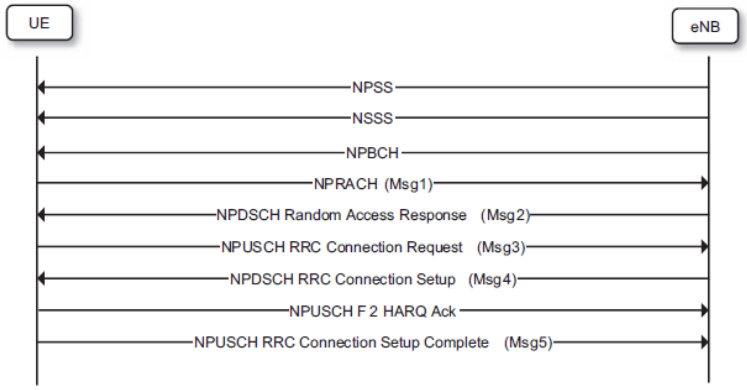

Fig. 1. NB-IoT Random Access Procedure. Initial steps of a UE to establish communication with an eNodeB.

3 Jamming the NB-IoT Synchronisation Process

The NB-IoT standard defines that NPSS and NSSS are transmitted in specific subframes on an 80 ms repetition interval. Both signals are designed to allow a device to use a unified synchronisation algorithm during initial acquisition without knowing the specific NB-IoT operation mode [6]. Therefore, to avoid collisions with LTE subframes, subframe 5 is used for the NPSS and subframe 9 is used for the NSSS. Also, in order to avoid a potential collision with the LTE Physical Downlink Control Channel (PDCCH), the subframes that carry NPSS or NSSS do not use the first three Orthogonal Frequency Division Multiplexing (OFDM) symbols. Thus, it leaves only 11 OFDM symbols per subframe available for NPSS and NSSS. The NPSS detection by the UE requires that the signal is detectable even with a very large frequency offset. Hence, all cells in an NB-IoT network use the same NPSS sequence. Consequently, a device only needs to search for one specific known NPSS sequence. Each of the 11 OFDM symbols in an NPSS subframe carries a copy of the base sequence. NB-IoT supports 504 unique NB-PCIDs indicated by the NSSS. Four different NSSS sequences are transmitted in an 80 ms repetition interval.

The NB-PCIDs is determined by a correlation algorithm using NPSS and NSSS which defines the peak correlation magnitude PEAK as the sum of the peak correlation magnitudes from time-domain NPSS detection and frequency-domain NSSS detection. PEAK is a scalar indicating the peak magnitude of the correlation used to detect a cell.

Adding a jamming signal to the NPSS and NSSS signal may have the effect that the correlation algorithm is still able to produce a result but the determined NB-PCIDs is incorrect. Jamming can be applied only to the NPSS and NSSS signal without the need to continuously jam the entire transmission channel.

4 Jamming Evaluation

To test the aforementioned jamming attack on the synchronisation signal, we use Matlab [7] with the LTE-Toolbox. The simulation fully synchronises, demodulates and decodes an NB-IoT downlink signal. A time-domain waveform of a Reference Measurement Channel (RMC) is generated for an NPDSCH; the Matlab class used for this purpose is *NBIoTDownlinkWaveformGenerator*. Then, we introduce a jamming signal generated using a downlink 4G RMC waveform where we can adjust the signal power. The resulting signal received by the UE is the sum of the generated signal obtained from the base station plus the jamming signal.

Following the example, the frequency offset estimation and correction are performed through the *lteFrequencyOffset* and *lteFrequencyCorrect* methods. Afterwards, OFDM demodulation and channel estimation are executed. Finally, to decode the MIB, the RE corresponding to the NPBCH from the first subframe across all receive antennas and channel estimates are extracted.

In our simulation, if the power of the interference signal is above 13dB a successful modification of the NB-PCIDs is observed. From the experiment results, it is observed that if the power on the jammer is insufficient, the communication with the specific eNodeB is inhibited because the UE is not able to decode the MIB and get the scheduling information.

Figure 2(a) shows the transmission signal without a jamming signal. Here, the cell ID is accurately detected [NNCellID: 120], and the MIB is decoded correctly. At this point, the MIB parameters are extracted (NNCellID, NB Reference Signal, Number of Sufbrame, HyperSuframe, Operation Mode, Additional Transmission SIB1).

In contrast, scenario Figure 2(b) shows the signal with jammer, where it is observed that it is not possible to decode the MIB, and a wrong cell ID is displayed [NNCellID: 371].

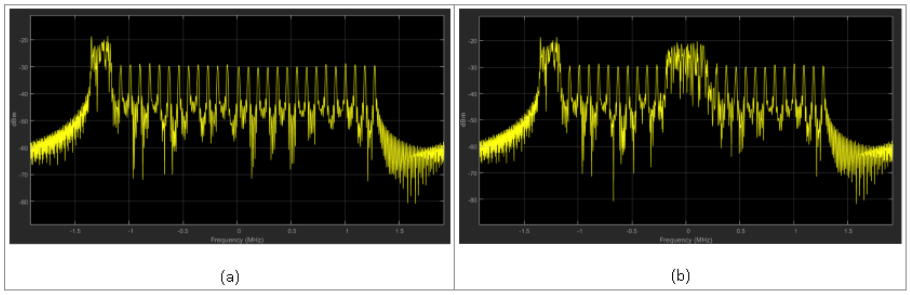

Fig. 2. Jamming Attack on NB-IoT: (a) Standard Transmission (b) Transmission with Jamming Signal.

5 Conclusions

We have shown that it is possible to interfere with the synchronisation signal used by NB-IoT devices (the UE) to establish communication with the base station. Thus, a simple selective jamming device can prevent communication of NB-IoT devices. Furthermore, our experiments indicate that careful design of the interference signal might enable an attacker to force the UE to recognise a specific NB-PCID. In our next steps, we will analyse how the jamming signal should be designed for this purpose. We also plan to investigate methods to detect the jamming of synchronisation signals and methods to make the detection of the NB-PCID more robust.

Acknowledgement

This publication has emanated from research conducted with the financial support of Science Foundation Ireland under Grant number 18/CRT/6222. For the purpose of Open Access, the author has applied a CC BY public copyright licence to any Author Accepted Manuscript version arising from this submission.

References

1. Third Generation Partnership Project, 3GPP., : Cellular system support for ultra-low complexity and low throughput Internet of Things (CIoT) (Release 13). In: Technical Specification Group GSM/EDGE Radio Access Network, 3GPP TR 45.820 V13.1.0. (2015)
2. Cao, J., Yu, P., Ma, M., Gao, W.: Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Network. In: IEEE Internet of Things Journal, vol. 6, pp. 1561–1575. (2019). https://doi.org/10.1109/JIOT.2018.2846803
3. Eygi, M., Karabulut-Kurt, G.: A Countermeasure against Smart Jamming Attacks on LTE Synchronization Signals. In: Journal of Communication, vol. 15, pp. 626–632. (2020).
4. Labib, M., Marojevic, V., Reed, J., Zaghloul, A.: How to enhance the immunity of LTE systems against RF spoofing. In: 2016 International Conference on Computing, Networking and Communications (ICNC), pp. 1–65. (2016). https://doi.org/10.1109/ICCNC.2016.7440650
5. Third Generation Partnership Project Standardization of NB-IoT Completed, https://www.3gpp.org/news-events/3gpp-news/. Last accessed 8 Jul 2021
6. Liberg, O., Sundberg, M., Wang, YO., Bergman, J., Sachs, J., Wikstrom, G. : Cellular Internet of Things from Massive Deployments to Critical 5G Applications. 2nd edn. (2020)
7. MATLAB: 9.7.0.1190202 (R2020b). The MathWorks Inc. Natick, Massachusetts. (2020)